PERCEPTUAL ENCRYPTION   P. OSCAR BOYKIN
AND DECRYPTION OF MOVIES   RICCARDO BOSCOLO

1   This is a continuation-in-part of an application filed

2   October 6, 2000 under Serial No. 09/684,724 and is a

3   continuation-in-part of an application filed December 19,

4   2000 under Serial No. 09/74,717.

5   BACKGROUND OF THE INVENTION

6   The invention relates to perceptual encryption of high

7   quality compressed video sequences and more particularly to

8   perceptual encryption of files of high quality video to

9   generate files of restricted video as perceptually encrypted

10   encoded data in an MPEG-1 format. The files of restricted

11   video can either be decoded and played as restricted video

12   or be decrypted, decoded and played as high quality video.

13   The MPEG standards determine the encoding and decoding

14   conditions of motion pictures in the form of a flow of video

15   digital data and a flow of audio digital data. The MPEG

1 standards define the encoding conditions of motion pictures,

2 whether associated or not with a sound signal, for storing

3 in a memory and/or for transmitting using Hertzian waves.

4 The MPEG standards also define the encoding conditions of

5 the individual picture sequences that form the motion

6 picture to be restored on a screen. Digital pictures are

7 encoded in order to decrease the amount of corresponding

8 data. Encoding generally uses compression techniques and

9 motion estimation. The MPEG standards are used to store

10 picture sequences on laser compact disks, interactive or

11 not, or on magnetic tapes. The MPEG standards are also used

12 to transmit pictures on telephone lines.

13   U. S. Patent No. 6,205,180 teaches a device which de-

14 multiplexes data encoded according to the MPEG standard in

15 the form of a data flow including system packets, video

16 packets and audio packets. The device independently

17 organizes according to the nature (system packets, video

18 packets and audio packets) of the data included in the

1   packets and the storing of the data in various registers.

2   The encoding and decoding conditions as defined by the

3   MPEG standards can be obtained from standard organizations.

4   The decoding of data encoded according to one of the MPEG

5   standards uses a separation of the data included in the data

6   flow according to its nature. The video data is separated

7   from the audio data, if any, and the audio and video data

8   are separately decoded in suitable audio and video decoders.

9   The data flow also includes system data. The system data

10   includes information relating to the encoding conditions of

11   the data flow and is used to configure the video and audio

12   decoder(s) so that they correctly decode the video and audio

13   data. The separation of the various data included in the

14   data flow is done according to their nature. The separation

15   is called the system layer. The system, audio and video data

16   are separated before the individual decoding of the audio

17   and video data.

18   There are current technologies for protecting the

3

1 copyright of digital media are based on a full encryption of

2 the encoded sequence. Full encryption does not allow the

3 user any access to the data unless a key is made available.

4   There are alternative approaches to ensure rights

5 protection. These approaches are based on "watermarking"

6 techniques which aim to uniquely identify the source of a

7 particular digital object thanks to a specific signature

8 hidden in the bit stream and invisible to the user.

9   The distribution of movies for viewing in the home is

10 one of the largest industries in the world. The rental and

11 sale of movies on videotape is a constantly growing industry

12 amounting to over $15 billion dollars in software sales in

13 the United States in 1995. The most popular medium for

14 distributing movies to the home is by videotape, such as

15 VHF. One reason for the robust market for movies on

16 videotape is that there is an established base of

17 videocassette recorders in people's homes. This helps fuel

18 an industry of local videotape rental and sale outlets

4

1 around the country and worldwide. The VHS videotape format

2 is the most popular videotape format in the world and the

3 longevity of this standard is assured due to the sheer

4 numbers of VHS videocassette players installed worldwide.

5 There are other mediums for distributing movies such as

6 laser disk and 8 mm tape. In the near future, Digital

7 Versatile Disk (DVD) technology will probably replace some

8 of the currently used mediums since a higher quality of

9 video and audio would be available through digital encoding

10 on such a disk. Another medium for distributing movies to

11 the home is through cable television networks. These

12 networks currently provide pay-per-view capabilities and in

13 the near future, direct video on-demand. For the consumer,

14 the experience of renting or buying the videotape is often

15 frustrating due to the unavailability of the desired titles.

16 Movie rental and sales statistics show that close to 50% of

17 all consumers visiting a video outlet store do not find the

18 title that they desire and either end up renting or buying

1   an alternate title or not purchasing anything at all. This

2   is due to the limited space for stocking many movie titles

3   within the physical confines of the store. With limited

4   inventory, video stores supply either the most popular

5   titles or a small number of select titles. Increasing the

6   inventory of movie titles is in direct proportion to the

7   shelf capacity of any one video-store. Direct video

8   distribution to the home is also limited by the availability

9   of select and limited titles at predefined times. Pay-per-

10   view services typically play a limited fare of titles at

11   predefined times offering the consumer a very short list of

12   options for movie viewing in the home. Video on-demand to

13   the home is limited by the cable television head end

14   facilities in its capacity to store a limited number of

15   titles locally. All of the aforementioned mechanisms for

16   distributing movies to the consumer suffer from inventory

17   limitations. An untapped demand in movie distribution

18   results if the inventory to the consumer can be made large

6

1 enough and efficient enough to produce movies-on-demand in

2 the format which the consumer desires. There is a need for

3 the ability to deliver movies on-demand with a virtually

4 unlimited library of movies on any number of mediums such as

5 VHS videotape, 8 mm videotape, recordable laser disk or DVD.

6 Some systems have addressed the need for distribution of

7 digital information for local manufacturing, sale and

8 distribution.

9 　　　　U. S. Patent No. 5,909,638 teaches system which

10 captures, stores and retrieves movies recorded in a video

11 format and stored in a compressed digital format at a

12 central distribution site. Remote distribution locations

13 are connected through fiber optic connections to the central

14 distribution site. The remote sites maybe of one of two

15 types: a video retail store or a cable television (CATV)

16 head end. In the case of a video retail store VHS videotapes

17 or any other format videotapes or other video media may be

18 manufactured on-demand in as little as three to five minutes

7

1   for rental or sell-through. In a totally automated

2   manufacturing system the customers can preview and order

3   movies for rental and sale from video kiosks. The selected

4   movie is either retrieved from local cache storage or

5   downloaded from the central distribution site for

6   manufacturing onto either a blank video-tape or a reused

7   videotape. One feature of the system is the ability to

8   write a two-hour videotape into a Standard Play (SP) format

9   using a high-speed recording device. A parallel compression

10   algorithm which is based on the MPEG-2 format is used to

11   compress a full-length movie into a movie data file of

12   approximately four gigabytes of storage. The movie data

13   file can be downloaded from the central site to the remote

14   manufacturing site and written onto a standard VHS tape

15   using a parallel decompression engine to write the entire

16   movie at high speeds onto a standard VHS videotape in

17   approximately three minutes.

18   U. S. Patent No. 5,793,980 teaches an audio-on-demand

8

1 communication system which provides real-time playback of

2 audio data transferred via telephone lines or other

3 communication links. One or more audio servers include

4 memory banks which store compressed audio data. At the

5 request of a user at a subscriber PC, an audio server

6 transmits the compressed audio data over the communication

7 link to the subscriber PC. The subscriber PC receives and

8 decompresses the transmitted audio data in less than real-

9 time using only the processing power of the CPU within the

10 subscriber PC. High quality audio data compressed according

11 to loss-less compression techniques is transmitted together

12 with normal quality audio data. Meta-data, or extra data,

13 such as text, captions, still images, etc., is transmitted

14 with audio data and is simultaneously displayed with

15 corresponding audio data. The audio-on-demand system also

16 has a table of contents which indicates significant

17 divisions in the audio clip to be played and allows the user

18 immediate access to audio data at the listed divisions.

9

1 Servers and subscriber PCs are dynamically allocated based

2 upon geographic location to provide the highest possible

3 quality in the communication link.

4 U. S. Patent No. 5,949,411 teaches a system which

5 previews movies, videos and music. The system has a host

6 data processing network connected via modem with one or more

7 media companies and with one or more remote kiosks to

8 transmit data between the media companies and the kiosks. A

9 user at a remote kiosk can access the data. A touch screen

10 and user-friendly graphics encourage use of the system.

11 Video-images, graphics and other data received from the

12 media companies are suitably digitized, compressed and

13 otherwise formatted by the host for use at the kiosk.

14 This enables movies, videos and music to be previewed at

15 strategically located kiosks. The data can be updated or

16 changed, as desired, from the host.

17 U. S. Patent No. 6,038,316 teaches an encryption module

18 and a decryption module for enabling the encryption and

10

1   decryption of digital information. The encryption module

2   includes logic for encrypting with a key the digital

3   information and distributing the digital information. The

4   decryption module includes logic for the user to receive the

5   key. The decryption logic then uses the key to make the

6   content available to the user.

7   U. S. Patent No. 6,097,843 teaches a compression

8   encoder which encodes an inputted image signal in accordance

9   with the MPEG standard.   The compression and decompression

10   different is from a main compression encoding which is

11   executed by a motion detection/compensation processing

12   circuit, a discrete cosine transforming/quantizing circuit,

13   and a Huffman encoding circuit. The compression and

14   decompression are executed by a signal compressing circuit

15   and a signal decompressing circuit. By reducing an amount

16   of information that is written into a memory provided in

17   association with the compression encoding apparatus, a

18   necessary capacity of the memory can be decreased.

11

1   U. S. Patent No. 6,064,748 teaches an apparatus for

2   embedding and retrieving an additional data bit-stream in an

3   embedded data stream, such as MPEG. The embedded data is

4   processed and a selected parameter in the header portion of

5   the encoded data stream is varied according to the embedded

6   information bit pattern. Optimization of the encoded data

7   stream is not significantly affected. The embedded

8   information is robust in that the encoded data stream would

9   need to be decoded and re-encoded in order to change a bit

10   of the embedded information. As relevant portions of the

11   header are not scrambled to facilitate searching and

12   navigation through the encoded data stream, the embedded

13   data can generally be retrieved even when the encoded data

14   stream is scrambled.

15   U. S. Patent No. 6,115,689 teaches an encoder and a

16   decoder. The encoder includes a multi-resolution transform

17   processor, such as a modulated lapped transform (MLT)

18   transform processor, a weighting processor, a uniform

1 quantizer, a masking threshold spectrum processor, an

2 entropy encoder and a communication device, such as a

3 multiplexor (MUX) for multiplexing (combining) signals

4 received from the above components for transmission over a

5 single medium. The decoder includes inverse components of

6 the encoder, such as an inverse multi-resolution transform

7 processor, an inverse weighting processor, an inverse

8 uniform quantizer, an inverse masking threshold spectrum

9 processor, an inverse entropy encoder, and an inverse MUX.

10   U. S. Patent No. 5,742,599 teaches a method which

11 supports constant bit rate encoded MPEG-2 transport over

12 local Asynchronous Transfer Mode (ATM) networks. The method

13 encapsulates constant bit rate encoded MPEG-2 transport

14 packets, which are 188 bytes is size, in an ATM AAL-5

15 Protocol Data Unit (PDU), which is 65,535 bytes in size.

16 The method and system includes inserting a plurality of

17 MPEG-2 transport packets into a single AAL-5 PDU, inserting

18 a segment trailer into the ATM packet after every two MPEG

13

1 packets, and then inserting an ATM trailer at the end of the

2 ATM packet. MPEG-2 transport packets are packed into one

3 AAL-5 PDU to yield a throughput 70.36 and 78.98 Mbits/sec,

4 respectively, thereby supporting fast forward and backward

5 playing of MPEG-2 movies via ATM networks.

6 　　　　U. S. Patent No. 6,157,625 teaches in an MPEG transport

7 stream, each audio signal packet is placed after the

8 corresponding video signal packet when audio and video

9 transport streams are multiplexed.

10 　　　　U. S. Patent No. 6,157,674 teaches an encoder which

11 compresses and encodes audio and/or video data by the MPEG-2

12 system, multiplexing the same and transmitting the resultant

13 data via a digital line. When generating a transport stream

14 for transmitting a PES packet of the MPEG-2 system, the

15 amounts of the compressed video data and the compressed

16 audio data are defined as whole multiples of the amount of

17 the transport packet (188 bytes) of the MPEG-2 system,

18 thereby to bring the boundary of the frame cycle of the

1 audio and/or video data and the boundary of the transport

2 packet into coincidence.

3   U. S. Patent No. 6,092,107 teaches a system which

4 allows for playing/browsing coded audiovisual objects, such

5 as the parametric system of MPEG-4.

6   The inventors incorporate the teachings of the above-

7 cited patents into this specification.

8 SUMMARY OF THE INVENTION

9   The present invention is generally directed to an

10 encoder and decoder. The encoder encodes a file of a high

11 quality video data in order to generate a file of video data

12 as encoded data. The decoder decodes the file of video data

13 as encoded data in order to regenerate the file of high

14 quality video data.

15   In a first separate aspect of the present invention, a

16 perceptual encryption module perceptually encrypts the

17 encoded data to generate restricted video data as

18 perceptually encrypted encoded data.

15

1   In a second separate aspect of the present invention, a

2 decryption module decrypts the perceptually encrypted

3 encoded data to generate encoded data.

4   Other aspects and many of the attendant advantages will

5 be more readily appreciated as the same becomes better

6 understood by reference to the drawing and the following

7 detailed description.

8   The features of the present invention which are

9 believed to be novel are set forth with particularity in the

10 appended claims.

11 DESCRIPTION OF THE DRAWINGS

12   Fig. 1 is a schematic drawing of the architecture of an

13 MPEG-1 program undergoing perceptual encryption to generate

14 a perceptually encrypted MPEG-1 stream according to the

15 present invention.

16   Fig. 2 is a schematic drawing of a diagram showing an

17 original video packet containing high fidelity video being

18 transformed into a new video packet containing low-fidelity

1 video data and an ancillary data containing encrypted

2 refinement data of Fig. 1 using an encrypton module and a

3 key.

4   Fig. 3 is a schematic drawing of a diagram showing

5 sequences of luminance and chrominance blocks in the 4:2:0

6 video format which are used in MPEG-1.

7   Fig. 4 is a schematic drawing of flow chart of the DCT

8 of the 8x8 block coefficients of the original video packet

9 of Fig. 2.

10   Fig. 5 is a schematic diagram of the 8x8 block

11 coefficients of the original video packet of Fig. 2 which is

12 divided into the low-fidelity video data and the ancillary

13 data.

14   Fig. 6 is a block diagram of perceptual encryption.

15   Fig. 7 is a schematic drawing of a standard MPEG-1

16 player which plays the perceptually encrypted MPEG-1 stream

17 of Fig. 1 as low fidelity video.

18   Fig. 8 is a schematic drawing of a standard MPEG-1

17

1 player which has a decryption module which with the use of

2 the key of Fig. 1 plays the perceptually encrypted MPEG-1

3 stream of Fig. 1 as high fidelity video according to the

4 present invention.

5 Fig. 9 is a block diagram of perceptual decryption.

6 DESCRIPTION OF THE PREFERRED EMBODIMENT

7 Referring to Fig. 1 in conjunction with Fig. 2 an MPEG-

8 1 program 10 includes multiplexed system packets 11, audio

9 packets 12 and video packets. The MPEG-1 program 10 is

10 encoded. The perceptual encryption system 20 includes a de-

11 multiplexing module 21, a system data buffer 22, an audio

12 data buffer 23, a video data buffer 24 and a multiplexing

13 module 25. The system data buffer 22, the audio data buffer

14 23 and the video data buffer 24 are coupled to the de-

15 multiplexing module 21. The multiplexing module 25 is

16 coupled to the system data buffer 22 and the audio data

17 buffer 23. The perceptual encryption system 20 also

18 includes a system data buffer 26,a main buffer 27, an

18

1 ancillary data buffer 28 and an encryption module 29 with a

2 key. The encryption module 29 is coupled to the ancillary

3 data buffer 28. U. S. Patent No. 6,038,316 teaches an

4 encryption module. The encryption module with a key enables

5 encryption of digital information. The encryption module

6 includes logic for encrypting the digital information and

7 distributing the digital information. U. S. Patent No.

8 6,052,780 teaches a digital lock which is encrypted it with

9 some n-bit key. In the case of a DES device the block size

10 is 64 bits and the key size is 56 bits. U. S. Patent No.

11 4,731,843 teaches a DES device in a cipher feedback mode of

12 k bits. The output of the multiplexing module 25 is a

13 perceptually encrypted MPEG-1 Program 30. The perceptually

14 encrypted an MPEG-1 program 30 includes multiplexed system

15 packets 11, audio packets 12 and low fidelity video packets

16 31 and refinement bit stream 32.

17   The overall architecture for perceptual encryption

18 includes a stream of the MPEG-1 program 10. The MPEG-1

19

1 program 10 is de-multiplexed, separating the system packets

2 11, the audio packets 12 and the audio packets 13. The

3 system packets 11 and the audio packets 12 are buffered in

4 the system data buffer 22 and the audio data buffer 23,

5 respectively, and transferred to the multiplexing module 25.

6   Referring to Fig. 1 the encoding strategy consists in

7 separating the spectral contained in the video sequence

8 across a first video sub-packet 41 and a second video sub-

9 packet 42. The second video sub-packet 42 containing the

10 refinement (high frequency) data is encrypted. To a decoder

11 the non-encrypted first video sub-packet 41 will appear as

12 the original video packet 13. The encrypted second video

13 sub-packet 42 is inserted in the stream as padding data.

14 This operation can be performed both in the luminance as

15 well as in the chrominance domain in order to generate a

16 variety of encoded sequences with different properties. It

17 is possible to build a video sequence where the basic low-

18 fidelity mode gives access to a low-resolution version of

20

1 the video sequence. The user is granted access to the full-

2 resolution version when he purchases the key. Perceptual

3 encryption is applicable to most video encoding standards,

4 since most of them are based on separation of the color

5 components (RGB or YCbCr) and use spectral information to

6 achieve high compression rates.

7   Perceptual encryption allows simultaneous content

8 protection and preview capabilities. It is safer than

9 watermarking since it prevents intellectual property rights

10 infringement rather than trying to detect it after the fact.

11 Perceptual encryption is applied to video encoded under the

12 MPEG-1 compression standard. The use of perceptual

13 encryption is not limited to this specific standard. It is

14 applicable to a large ensemble of audio/video compression

15 standards, including MPEG-2, MPEG-4, MPEG-21, MPEG-7,

16 QuickTime, Real Time, AVI, Cine Pak and others.

17   Referring to Fig. 3 an 8x8 pixel image area represents

18 the basic encoded unit in the MPEG-1 standard. Each pixel

21

1   is described by a luminance term (Y) and two chrominance

2   terms (Cb and Cr). The only video format which the MPEG-1

3   standard supports is the 4:2:0 format. The chrominance

4   resolution is half the luminance resolution both

5   horizontally and vertically. As a consequence compressed

6   data always presents a sequence of four luminance blocks

7   which are followed by two chrominance blocks.

8   Referring to Fig. 4 a flow chart of the transformation

9   from an 8x8 region to 8x8 DCT of each component is computed

10 thereby returning 64 coefficients per component. The

11 coefficients of each component are sorted in order of

12 increasing spatial frequency.

13   Referring to Fig. 5 in conjunction with Fig. 6 as the

14 input bit stream is being parsed, a video packet 13 is

15 identified and its 8x8 DCT coefficients are selectively sent

16 to either a main buffer 27 or an ancillary buffer 28 in

17 order to generate the low-resolution data for the main video

18 packet 31 or the ancillary data for the refinement bit

22

1   stream 32, respectively. The parameters MaxYCoeffs,

2   MaxCbCoeffs and MaxCrCoeffs allow the content provider to

3   select the maximum number of Y, Cb and Cr coefficients,

4   respectively, to be retained in the original bit stream. As

5   soon as the maximum number of coefficients in the main video

6   packet 31 for a given component is reached, an end-of-block

7   (EOB) code is appended to signal the end of the current

8   block. This is a crucial step since the Huffman encoded 8x8

9   blocks do not present any start-of-block marker and the EOB

10   sequence is the only element signaling the termination of

11   the compressed block and the beginning of the next. There

12   are two different types of 8x8 data blocks encountered in

13   the MPEG-1 standard. The first type occurs in I-pictures,

14   which consist of frames where no motion prediction occurs.

15   In these frames each 8x8 image region is compressed using a

16   modified JPEG algorithm and the DCT of each of the

17   components is encoded directly (intra-frame compression).

18   In P-pictures and B-pictures, instead, one-directional or

23

1 bi-directional motion-compensated prediction takes place to

2 exploit the temporal redundancy of the video sequence. In

3 these frames either some or all of the 8x8 image blocks are

4 estimated from the neighboring frames and the prediction

5 error is encoded using a JPEG style algorithm (inter-frame

6 compression). Several strategies for applying different

7 low-pass filters to intra-coded or inter-coded blocks were

8 explored. The optimal solution applies identical low-pass

9 filtering to both types of encoded blocks. The theoretical

10 explanation of this result resides in the superposition-

11 principle. It is a consequence of the fact that the DCT is

12 a linear operator.

13   Referring to Fig. 6 in conjunction with Fig. 2 once the

14 video packet 13 parsing is complete, the first video sub-

15 packet 31 which is stored in the main buffer 27 is released

16 to the output stream to replace the original video packet

17 13. The refinement video sub-packet 32 is encrypted and the

18 stored in the ancillary data buffer 28 to be released to the

24

1   output as a padding stream. The function of the padding

2   stream is normally that of preserving the current bit rate.

3   Since the size of the combined first and second video sub-

4   packets 31 and 32 is only slightly larger than the original

5   video packet 13 the bit rate of the original sequence is

6   preserved and the decoding of the encrypted sequence does

7   not require additional buffering capabilities. A heading-

8   generator generates a specific padding packet header. The

9   padding heading is used to insert the encrypted ancillary

10   data 32 into the video stream. This allows full

11   compatibility with a standard decoder since this type of

12   packet is simply ignored by the decoder. A proprietary 32-

13   bit sequence is inserted at the beginning of the ancillary

14   data to allow the correct identification of the encrypted

15   video sub-packets 32. Moreover since no limit on the size

16   of the video packets 13 is imposed with the exception of

17   buffering constraints additional data, such as decryption

18   information, can be included at any point inside these

1 packets.

2   In another embodiment perceptual encryption decomposes

3 each of the video packet 13 into several sub-packet. The

4 first sub-packet provides the essential conformance to the

5 standard and contains enough information to guarantee a

6 basic low-fidelity viewing capability of the video sequence.

7 The first video sub-packet is not subject to encryption.

8 Each of the second video sub-packet and all subsequent video

9 sub-packets represents a refinement bit stream and, when

10 added incrementally, serially enhances the "quality" of the

11 basic video packet until a high fidelity video sequence is

12 obtained. Each video sub-packet is encrypted and are placed

13 back in the bit stream as padding streams. The standard

14 MPEG-1 decoder will ignores padding streams.

15   The definition of "successive levels of quality" is

16 arbitrary and is not limited to a particular one. Possible

17 definitions of level of fidelity are associated with, but

18 are not restricted to, higher resolution, higher dynamic

26

1   range, better color definition, lower signal-to-noise ratio

2   or better error resiliency. The video packets 13 are

3   partially decoded and successively encrypted.

4   The main idea behind the perceptual encryption is to

5   decompose each video packet 13 into at least two video sub-

6   packets. The first video sub-packet 31 is the basic video

7   packet and provides the basic compliance with the standard

8   and contains enough information to guarantee low-fidelity

9   viewing capabilities of the video sequence. The first video

10 sub-packet 31 is not subjected to encryption and appears to

11 the decoder as a standard video packet. The second video

12 sub-packet 32 represents a refinement bit stream and is

13 encrypted. The refinement bit stream enhances the "quality"

14 of the basic video packet and when combined with the first

15 video sub-packet 31 is able to restore a full fidelity video

16 sequence. The second video sub-packet 32 is encrypted using

17 the encryption module 29 and the key. Perceptual encryption

18 includes the use of standard cryptographic techniques. The

27

1 encrypted second video packet 32 is inserted in the bit

2 stream as padding data and is ignored by the standard MPEG-1

3 decoder.

4   Perceptual encryption encrypts high quality compressed

5 video sequences for intellectual property rights protection

6 purposes. The key part of perceptual encryption resides in

7 its capability of preserving the compatibility of the

8 encrypted bit stream with the compression standard. This

9 allows the distribution of encrypted video sequences with

10 several available levels of video and audio quality

11 coexisting in the same bit stream. Perceptual encryption

12 permits the content provider to selectively grant the user

13 access to a specific fidelity level without requiring the

14 transmission of additional compressed data. The real-time

15 encryption for compressed video sequences preserves the

16 compatibility of the encrypted sequences with the original

17 standard used to encode the video and audio data. The main

18 advantage of perceptual encryption is that several levels of

28

1   video quality can be combined in a single bit stream thereby

2   allowing selective restriction access to the users. When

3   compared to other encryption strategies perceptual

4   encryption presents the advantage of giving the user access

5   to a "low fidelity" version of the audio-video sequence,

6   instead of completely precluding the user from viewing the

7   sequence.

8   Since perceptual encryption acts on the video packets

9   13, as they are made available, encryption can be performed

10 in real-time on a streaming video sequence with no delay.

11 This result is from the fact that each video packet 13 is

12 perceptually encrypted separately and the refinement bit

13 streams for a specific video packet are streamed immediately

14 following the non-encrypted low fidelity data. This feature

15 is very attractive because it makes it suitable for real-

16 time on demand streaming of encrypted video. Moreover

17 keeping perceptual encryption distributed gives the encoded

18 sequences better error resiliency properties, allowing

29

1 easier error correction. In order to keep the overhead

2 introduced by perceptual encryption as small as possible, no

3 extra information related to the refinement sub-packets is

4 added to the video packet header.

5   Referring to Fig. 7 a standard MPEG-1 player 110

6 includes a de-multiplexing module 111, a system data buffer

7 112, an audio data buffer 113, a low fidelity video data

8 buffer 114, a refinement bit stream data buffer 115, an

9 audio decoder 116, a video decoder 117, a synchronizer 118,

10 and a display 119. The system data buffer 112, the audio

11 data buffer 113, the low fidelity video data buffer 114 and

12 the refinement bit stream data buffer 115 are coupled to the

13 de-multiplexing module 111. The synchronizer 118 is coupled

14 to the system data buffer 112 and the audio data buffer 113.

15 The video decoder 117 is coupled to the low fidelity video

16 data buffer 114. The synchronizer 118 is also coupled to

17 the video decoder 117. The video decoder 117 may include a

18 Huffman decoder and an inverse DCT, motion compensation and

1   rendering module. The display 119 is coupled to the inverse

2   DCT, motion compensation and rendering module.

3   The standard MPEG-1 player 110 performs the input stream

4   parsing and de-multiplexing along with all of the rest of

5   operations necessary to decode the low fidelity video

6   packets including the DCT coefficient inversion, the image

7   rendering as well as all the other non-video related

8   operations.

9   Referring to Fig. 8 in conjunction with Fig. 9 an MPEG-

10   1 player 210 includes a de-multiplexing module 211, a system

11   data buffer 212, an audio data buffer 213, a low fidelity

12   video data buffer 214, a refinement bit stream data buffer

13   215, an audio decoder 216, a Huffman Decoder and Perceptual

14   Decryptor Plug-in 217, an inverse DCT, motion compensation

15   and rendering module 218, a synchronizer 219 and a display

16   220. The system data buffer 212, the audio data buffer 213,

17   the low fidelity video data buffer 214 and the refinement

18   bit stream data buffer 215 are coupled to the de-

1   multiplexing module 211. The audio decoder 216 is coupled

2   to the audio data buffer 213. The synchronizer 219 is

3   coupled to the system data buffer 212 and the audio decoder

4   216. The Huffman decoder and perceptual encryptor Plug-I

5   217 is coupled to the low fidelity video data buffer 214 and

6   the refinement bit stream data buffer 215. The inverse DCT,

7   motion compensation and rendering module 218 is coupled to

8   the Huffman Decoder and Perceptual Decryptor Plug-in 217.

9   The synchronizer 218 is also coupled to the inverse DCT,

10   motion compensation and rendering module 218. The display

11   220 is coupled to the synchronizer 218. The Huffman decoder

12   and Perceptual Encryptor plug-in 217 performs the input

13   stream parsing and de-multiplexing for the MPEG-1 player

14   210. The MPEG-1 player 210 performs all of the rest of

15   operations necessary to decode the low fidelity video

16   packets including the DCT coefficient inversion, the image

17   rendering, as well as all the other non-video related

18   operations. The plug-in may be designed to handle

32

1   seamlessly MPEG-1 sequences coming from locally accessible

2   files as well as from streaming video. U. S. Patent No.

3   6,038,316 teaches a decryption module. The decryption

4   module enables the encrypted digital information to be

5   decrypted with the key. The decryption module includes

6   logic for decrypting the encrypted digital information. The

7   standard MPEG-1 player 210 is coupled to a display 214. The

8   plug-in replaces the front-end of the MPEG-1 player and

9   performs the input stream parsing and de-multiplexing. The

10 plug-in carries on all the operations necessary to decode

11 the video packets 31 and 32 and perform decryption.

12 Similarly to perceptual encryption decryption acts on one

13 video packet at the time. Once the current video packet is

14 buffered the system searches for its refinement sub-packets

15 that immediately follow the main packet. According to the

16 level of access to the video sequence granted to the user,

17 the available refinement bit streams are decrypted and are

18 combined with the original packet. The fusion of the main

33

1   packet 31 with the refinement sub-packets 32 takes place at

2   the block level. In decryption only additional spectral

3   information is contained in the refinement data. This

4   implementation represents a possible example of definition

5   of multiple level of access to the video sequence, but

6   decryption is not limited to a particular one.

7   The encrypted bit streams contain refinement DCT

8   coefficients whose function is to give access to a full-

9   resolution high fidelity version of the video sequence. The

10   fusion of the original block data with the refinement

11   coefficients is possible with minimal overhead using the

12   following process. Given an 8x8 image block, the Huffman

13   codes of the main packet are decoded until an end-of-block

14   sequence is reached. At this point the decrypting module

15   211 starts decoding the Huffman codes of the next refinement

16   packet, if any is available. The DCT coefficients are then

17   appended to the original sequence until the EOB sequence is

18   read. Decryption continues until all the refinement packets

1   are examined. In the special case of an additional sub-

2   packet that does not contain any additional coefficient for

3   the given 8x8 block, an EOB code is encountered immediately

4   at the beginning of the block, signaling the Huffman Decoder

5   and Perceptual Decryptor Plug-in 217 that no further DCT

6   coefficients are available.

7   In the implementation of decryption for the MPEG-1

8   standard player, the encrypted bit streams contain

9   refinement DCT coefficients whose function is to give access

10   to a full-resolution high fidelity version of the video

11   sequence. The fusion of the original block data with the

12   refinement coefficients is possible with minimal overhead

13   using the following process. Given an 8x8 image block, the

14   Huffman codes of the main packet are decoded until an end-

15   of-block sequence is reached. At this point the decrypting

16   module starts decoding the Huffman codes of the next

17   refinement packet, if any is available. The DCT

18   coefficients are then appended to the original sequence

35

1   until the EOB sequence is read. Decryption continues until

2   all the refinement packets are examined. In the special

3   case of an additional sub-packet that does not contain any

4   additional coefficient for the given 8x8 block, an EOB code

5   is encountered immediately at the beginning of the block,

6   signaling the Huffman Decoder and Perceptual Decryptor Plug-

7   in 217 that no further DCT coefficients are available.

8   Similarly to the perceptual encryption the decryption

9   takes place independently on each video packet, allowing

10   real-time operation on streaming video sequences. As soon as

11   all the refinement sub-packets, following the principal

12   packet, are received, decryption can be completed.

13   A technology for encrypting high quality compressed video

14   sequences for rights protection purposes resides in its

15   capability of preserving the compatibility of the encrypted

16   bit stream with the compression standard. The technology

17   allows the distribution of encrypted video sequences with

18   several available levels of video and audio quality

36

1   coexisting in the same bit stream. The technology permits

2   to selectively grant the user access to a specific fidelity

3   level without requiring the transmission of additional

4   compressed data. The technology is a real-time

5   encryption/decryption technique for compressed video

6   sequences. The technology preserves the compatibility of

7   the encrypted sequences with the original standard used to

8   encode the video and audio data. The main advantage of the

9   technology is that several levels of video quality can be

10   combined in a single bit stream allowing selective access

11   restriction to the users. When compared to other common

12   encryption strategies implementation of the technology

13   presents the advantage of giving the user access to a "low

14   fidelity" version of the audio-video sequence, instead of

15   completely precluding the user from viewing the sequence.

16   The description of the technology has focused on the

17   MPEG-1 standard in order to provide a detailed description

18   of the technology. See ISO/IEC 11172-1:1993 Information

1 Technology-Coding of Moving Pictures and Associated Audio

2 for Digital Storage Media up to about 1,5 Mbit/s-Part

3 1:Systems, Part 2: Video. The scope of technology is not

4 limited to this specific standard. The technology is

5 applicable to a large ensemble of audio/video compression

6 standards. See V. Bhaskaran and K. Konstantinides. Image

7 and Video Compression Standards: Algorithms and

8 Architectures. Kluwer Academic Publishers, Boston, 1995.

9   In the MPEG-1 standard a high compression rate is

10 achieved through a combination of motion prediction

11 (temporal redundancy) and Huffman coding of DCT (Discrete

12 Cosine Transform) coefficients computed on 8x8 image areas

13 (spatial redundancy). See J.L. Mitchell, W.B. Pennebaker,

14 C.E. Fogg and D.J. LeGall. MPEG Video Compression Standard.

15 Chapman & Hall. International Thomson Publishing, 1996. One

16 of the most important features of the DCT is that it is

17 particularly efficient in de-coupling the image data. As a

18 consequence the resulting transformed blocks tend to have a

38

1   covariance matrix that is almost diagonal, with small cross-

2   correlation terms. The most relevant feature to the

3   technology, though, is that each of the transform

4   coefficients contains the information relative to a

5   particular spatial frequency. As a consequence cutting part

6   of the high frequency coefficients acts as a low-pass filter

7   decreasing the image resolution.

8   From the foregoing it can be seen that perceptual

9   encryption and decryption of movies have been described.

10   Accordingly it is intended that the foregoing

11   disclosure and drawings shall be considered only as an

12   illustration of the principle of the present invention.